LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

TOIMIPISTEEN TIETOVERKON SUUNNITTELU

Case: TMT. Malinen Oy / Vuoripoika Oy

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Tuomo Meckelburg

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

MECKELBURG, TUOMO:

Toimipisteen tietoverkon suunnittelu
TMT. Malinen Oy / Vuoripoika Oy

Tietoliikennetekniikan opinnäytetyö, 40 sivua

Kevät 2015

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli kehittää kohdeyrityksenä olevan Vuoripoika Oy:n tietoverkon tehokkuutta ja toimivuutta. Tavoitteena oli selvittää toteutustapa Site-to-Site VPN -yhteyden perustamiselle TMT. Malinen Oy:n lähiverkkoon ja antaa siitä ratkaisuehdotus kohdeyritykselle.

Lähtökohtana oli selvittää yrityksen tarpeet sekä se, mitä tulevalta tietoverkolta vaadittaisiin. Tällä hetkellä Vuoripoika Oy:ssä VPN-yhteys yhtiön lähiverkkoon oli toteutettu Remote Access -yhteydellä yksittäisiltä tietokoneilta.

Toisistaan erillä olevien tietoverkkojen tietoturvaan kuuluu suojattu VPN-yhteys tietoverkkojen välillä. Lähiverkkojen välille muodostetun turvallisen yhteyden päätelaitteina oleva palomuuri estää virusten pääsyn lähiverkkoon ja ehkäisee verkon kautta tapahtuvan luvattoman sekä näkymättömän käytön. Päätelaitteessa toimiva NAT konvertoi IP-osoitteet ja suojaa sisäverkkoa ohjaamalla sisäverkon verkkoliikenteen ulkoverkkoon päin yhden IP-osoitteen taakse.

Kohdeyrityksen ja yhtiön välille tuli suunnitella VPN-yhteys, joka olisi monistettavissa tai siirrettävissä helposti. Tästä syystä työssä on keskitytty langattomien ratkaisujen vertailuun. Työn tarkoituksena on antaa kohdeyritykselle tarvittavat tiedot, joiden perusteella se pystyy harkitsemaan tietoverkkonsa laajentamista.

Työssä käsitellään kahta ratkaisuvaihtoehtoa Site-to-Site VPN-yhteyden toteutukseen. Suositeltu ratkaisu rakennettaisiin olemassa olevan internetyhteyden päälle palomuuri-päätelaitteella ja vaihtoehtoisessa ratkaisussa VPN-yhteys muodostettaisiin siihen soveltuvassa ADSL-modeemissa. Kummassakin ratkaisussa käytettäisiin langattomia WLAN-tukiasemia internetyhteyden jakamiseen.

Asiasanat: VPN, tietoverkko

Lahti University of Applied Sciences
Faculty of Technology

MECKELBURG, TUOMO: Design of a office network
TMT. Malinen Oy / Vuoripoika Oy

Bachelor's Thesis in Telecommunications Technology, 40 pages

Spring 2015

ABSTRACT

The purpose of this Bachelor's thesis was to enhance the effectiveness and functionality of the computer network of the target company Vuoripoika Oy. The objective was to study how to implement a Site-to-Site VPN connection to the local area network TMT. Malinen Oy and give a solution proposal to the target company.

The starting point was to determine the needs of the Vuoripoika and what would be required of the network. At the moment in Vuoripoika, the VPN connection to the Malinen´s local area network has been implemented as a Remote Access connection from individual computers.

A protected VPN connection is part of information security between two separate networks. Firewalls, which function as endpoints for the safe connection between the local area networks stop viruses from entering the local network and prevent unauthorized or invisible use from the internet. NAT on the endpoint device converts IP addresses and protects the internal network by diverting all traffic from the local area network to the outside network, behind one IP address.

It was necessary to design an easily moved or replicated VPN connection between the Vuoripoika and the Malinen. For this reason this work focuses on evaluation of wireless solutions. The purpose of the work is to offer the target company necessary information so that they are able to consider expanding their communications network.

The work deals with two different solutions for the creation of a Site-to-Site VPN. The suggested solution would be built on top of an existing internet connection with a separate firewall endpoint device and the alternate solution would form the VPN connection within a suitable ADSL modem. In both cases wireless access points would be used to share the internet connection.

Key words: VPN, networking

SISÄLLYS

LYHENNELUETTELO

802.11	IEEE:n standardoima WLAN-standardi
ADSL	Asymetric Digital Subscriber Line, puhelinlinjaa käyttävä verkkokytkintekniikka
Access Point	Langaton tukiasema
IPsec	IP Security Architecture, joukko TCP/IP-tietoliikenneprotokollia
IP	Internet Protocol, vastaa päätelaitteiden osoitteista ja pakettien reitittämisestä verkossa
Korppu	Levyke, magneettinen muistilevy
LAN	Local Area Network, lähiverkko
LMSG	LAN/MAN Standardization Group
Malware	Haittaohjelma
MAN	Metropolitan Area Network, IEEE 802.16 -standardin mukainen alueverkko
Messagelabs	Turvallisuusratkaisuja tarjoava yritys
NAT	Network Address Translation, osoitteenmuunnostekniikka
SSL	Secure Sockets Layer, salausprotokolla, tunnetaan nykyisin nimellä TLS
System File	Tiedostojärjestelmä
TLS	Transport Layer Security, salausprotokolla, jolla suojataan internetsovellusten tietoliikenne IP-verkkojen yli.
OSI-malli	Open Systems Interconnection Reference Model, tiedonsiirtoprotokollien yhdistelmä, kuvattuna seitsemässä tasossa

RAN	Range Area Network, alueverkko
RAT	Remote Access Trojan, haittaohjelma, joka käyttää etäkäyttöä
SPAM	Roskaposti sähköpostiin
Proxy	Välityspalvelin, välittää ja suodattaa verkossa siirrettäviä tiedostoja
VDSL	Very high speed Digital Subscriber Line, puhelinlinjaa käyttävä verkkokytkintekniikka
VPN	Virtual Private Network, virtuaalinen yksityisverkko
WAN	Wide Area Network, laajaverkko
WEP	Wired Equivalent Pricavy, vanha salausjärjestelmä WLAN-verkossa
WDS	Windows Deployment Services, ohjelmisto Windows-käyttöjärjestelmien etäasennukseen, tai Wireless Distribution System, järjestelmä langattomien tukiasemien yhteenliittämiseen
WiFi/Wi-Fi	Wireless Fidelity, standardin 802.11 mukainen WLAN
WPA/2	Wi-Fi Protection Access, salausjärjestelmä WLAN-verkossa
WLAN	Wireless Local Area Network, langaton verkko

1 JOHDANTO

Opinnäytetyön tarkoituksena on vertailla erilaisia ratkaisuja, joilla lähiverkkoa voidaan kustannustehokkaasti laajentaa ja yhdistää fyysisesti erillään oleviin toimitiloihin. Työssä vertaillaan erilaisia ratkaisumalleja ja pyritään antamaan tiedot, joilla kohdeyritys voisi sekä tietoturvallisesti laajentaa lähiverkkoaan tytäryhtiön tuotantotiloihin.

Kohdeyritys, TMT. Malinen Oy, on yksi Suomen johtavista ja monipuolisimmista kuljetuskaluston päällysrakenneosien valmistajista sekä toimittajista. TMT. Malisen tytäryhtiö Vuoripoika Oy on metallin ja muovin jatkojalostukseen keskittynyt yritys. Laajan oman tuotannon lisäksi TMT. Malinen Oy on luonut kansainvälisen yhteistyöverkoston varmistamaan asiakkailleen kattavan palvelukokonaisuuden. (TMT. Malinen Oy 2014.)

TMT. Malinen Oy:n lähiverkkoa ei ole jaettu tytäryhtiöille, mutta yhteys lähiverkkoon saadaan yksittäiseltä tietokoneelta Remote Access VPN -yhteyden avulla. Tuotannonohjausjärjestelmän sekä verkkolevyjen käytön tehostamiseksi on järkevää laajentaa lähiverkko toimimaan myös tytäryhtiöissä. Opinnäytetyössä tutkitaan erilaisia vaihtoehtoja lähiverkon laajentamiseen tytäryhtiö Vuoripoika Oy:n tiloihin. Opinnäytetyö käsittelee myös tietoturvaa sekä lähiverkon laajentamisen tuomia etuja.

2 TIETOVERKKO

2.1 Yleistä tietoverkosta

Verkolla tarkoitetaan kaapelien, radiotien tai valoyhteyden avulla toisiinsa liitettyjä tietokonelaitteita, jotka pystyvät ottamaan yhteyden toisiinsa verkon avulla. Tämän lisäksi verkossa toimiva verkkolaite välittää dataa ja toimii päätelaitteena tai muiden verkkolaitteitten liitäntäpisteenä. Verkkolaitteitten ja niissä olevien ohjelmistojen avulla voidaan hallita datan liikkumista verkossa. Kaapelointi luo puitteet yhteyden muodostamiselle, mutta verkko tarvitsee toimiakseen myös erilaisia ohjelmistoja, jotka määrittelevät liikennöinnin verkossa. (Jaakohuhta 2005, 4–5.)

Verkot voidaan jakaa kolmeen eri kokonaisuuteen:

- Lähiverkko eli LAN on pienen alueen ja suuren tiedonsiirtokapasiteetin omaava verkko.

- Alueverkko on nimitys verkoista, jotka on rakennettu kaupungin, kuntayhtymän, yliopiston tai jonkin taajama-alueen kattaviksi. Alueverkosta voidaan käyttää IEEE803.6-standardin mukaisesti nimitystä MAN (*Metropolitan Area Network*) tai nykyisin käytössä olevaa nimitystä RAN (*Range Area Network*), jotka tarkoittavat käytännössä samaa.

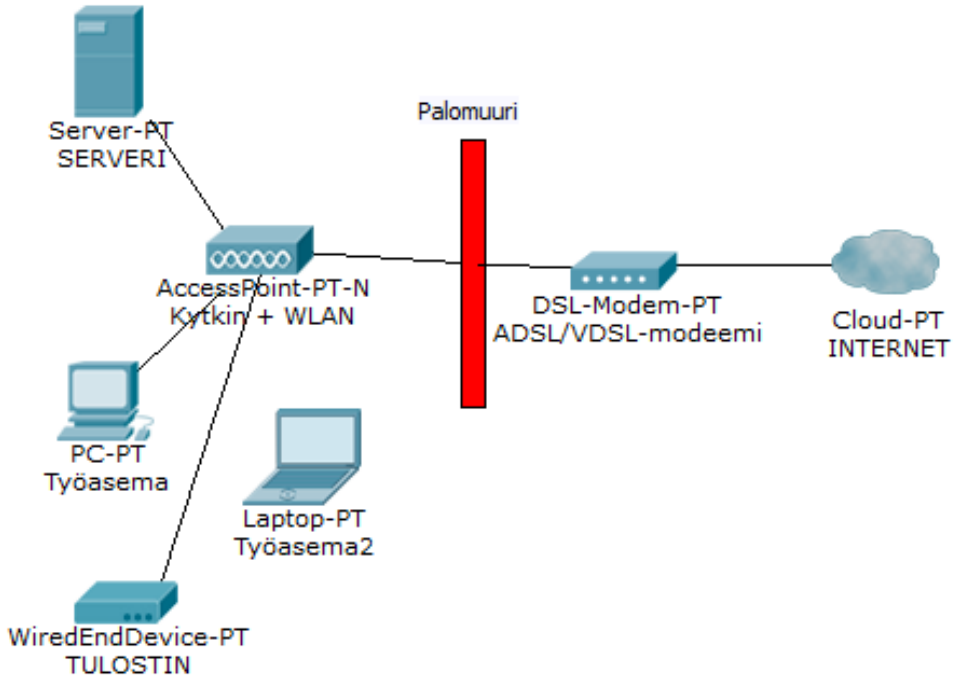
- Laajaverkko eli WAN (*Wide Area Network*) ulottuu yleensä paikkakunnalta toiselle ja maan rajojen ulkopuolelle aina maan osien väliseksi verkoksi. Laajaverkko voi yhdistää lähiverkkoja, joita teleoperaattori toteuttaa erilaisilla tekniikoilla. (Jaakohuhta 2005, 4–5.)

2.2 Lähiverkko

Lähiverkko (kuvio 1) eli LAN on sisäistä tietoliikennettä toteuttava ja suuren tiedonsiirtokapasiteetin omaava verkko, joka on yleensä yhden organisaation hallinnassa. Lähiverkko voi myös olla kokonaan tai osittain langaton WLAN-

verkko (*Wireless LAN*). Lähiverkon ylläpidon voi hoitaa ulkopuolinen taho, joka huolehtii lähiverkosta yrityksen puolesta. (Jaakohuhta 2005, 4.)

Lähiverkot on alun perin tarkoitettu rajallisen alueen käyttöön, mutta niitä käytetään nykyään yhtä hyvin kotiverkoissa kuin alueverkoissakin. Työasemat voidaan liittää verkkoon kaapeliyhteydellä tai yhä useammin WLAN-radioyhteydellä. (Tallinna Ülikooli 2014.)



KUVIO 1. Esimerkki lähiverkosta

2.3 Etherhet ja CSMA/CD

Ethernet on kehittynyt 30 vuoden aikana radioteitse toteutetusta 4 800 bittiä sekunnissa kulkevasta siirtotekniikasta 10 000 megabittiä sekunnissa välittävään valokuitusiirtotekniikkaan. Ethernet on maailman yleisin lähiverkkotekniikka ja

vallitseva tekniikka myös alueverkoissa. Kesäkuussa 1981 IEEE perusti 802.3-alikomitean, jonka tavoitteena oli tuottaa Ethernet-standardi, joka olisi kansainvälisesti hyväksyttävä. Nykyisin Ethernet ja 802.3 tarkoittavatkin samaa asiaa. (Jaakohuhta 2005, 9, 14.)

Tiedonsiirto Ethernet-verkoissa perustuu yksinkertaiseen CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) -menettelyyn. Se tarkoittaa sitä, että verkkoa kuunnellaan ensin päätelaitteella (*carrier sense*), ja jos verkossa ei havaita liikennettä, voidaan sanoma lähettää (*multiple access*). Verkkoon voi lähettää sanomia vain yksi laite kerrallaan. Joskus voi käydä myös niin, että kaksi laitetta lähettää yhtä aikaa sanomia, jolloin seuraa sanomien yhteentörnäys (*collision*). Törmäyksen havainnut asema (*collision detection*) vahvistaa törmäyksen ja osapuolet arpovat uuden lähetysajan IP-paketeille. Verkkoon ei voi lähettää uusia IP-paketteja, ennen kuin edelliset lähetykset on toimitettu ja siirtotie on tyhjä. (Jaakohuhta 2005, 90.)

2.4 Kaapelointi

Eurooppalainen yleiskaapelointistandardi EN50173 määrittää kaapeliluokat ja kaapelointitavat. Yleiskaapelointistandardi EN50173 määrittää myös kaistanleveydet ja kaapeleille asetetut testausarvot (Wikipedia 2014d). Kaapeliluokat jaetaan kahdeksaan kategoriaan, ja yleisesti käytössä ovat kategorian 5 tai 6 kaapelit (taulukko 1).

Yleisin liitintyyppi parikaapelille on lähiverkossa käytetty RJ-45. Ethernet- ja puhelinverkossa käytetään yleisimmin suojaamatonta parikaapelia (UTP), koska suojaamaton kaapeli on edullinen. Parisuojattua STP-kaapelia käytetään, kun suojaukseen on erityinen tarve, kuten voimavirtakaapelien tai muuntajien läheisyydessä. (Wikipedia 2014d.)

TAULUKKO 1. Parikaapelit (Wikipedia 2014d)

Parikaapelit	Sovellukset	100BASE-TX	1000BASE-T	10GBASE-T
Kategoria	Kaistan leveys			
Cat5	100 MHz	X	X	
Cat5e	100 MHz	X	X	
Cat6	250 MHz	X	X	
Cat6a	250 MHz	X	X	X

2.5 Internetyhteysmuodot

Internetyhteyden voi muodostaa monella eri tavalla, mutta näistä yleisimmät ovat DSL-, kaapeli-, valokuitu-, WLAN- ja matkaviestinverkkoyhteydet. Kiinteistä yhteyksistä lankapuhelinverkkoa käyttävät DSL-yhteydet ovat suosituimpia.

ADSL hyödyntää kiinteää puhelinverkkoa, mutta käyttää eri taajuusaluetta kuin perinteinen lankapuhelin. ADSL-yhteys tarjoaa käyttäjälleen oman kaistan, jota ei jaeta alueen muiden käyttäjien kanssa, ja tällöin yhteysnopeus ei riipu muista käyttäjistä. Yhteys käyttäjän ja palvelun tarjoajan välille muodostetaan ADSL-modeemin avulla, ja lopulliseen yhteysnopeuteen vaikuttaa käyttäjän etäisyys paikallisvaihteesta. ADSL-yhteyksissä maksiminopeus sisäänpäin on 24 Mb/s ja ulospäin 3 Mb/s. (Suomicom 2014.)

VDSL-yhteys perustuu ADSL:n tapaan kiinteään puhelinverkkoon, mutta VDSL varaa myös lankapuhelinkaistan tiedonsiirtoon, jolloin lankapuhelinta ei voida käyttää samanaikaisesti. VDSL-yhteyden nopeuteen vaikuttavat käyttäjän etäisyys paikallisvaihteesta, puhelinkaapelin paksuus ja käytettävä nopeusprofiili. VDSL2-yhteyksissä saavutetaan maksimissaan 100 Mb/s sisäänpäin ja 100 Mb/s ulospäin. (Suomicom 2014.)

SHDSL-yhteys on symmetrinen tiedonsiirtotapa, jolla latauksen (*download*) ja paluun (*upload*) yhteysnopeus on sama. SHDSL-yhteydellä voidaan saavuttaa 11,4 megabitin sekuntinopeus lataus- ja paluuliikenteelle. (Wikipedia 2014e.)

Kaapelimodeemi toimii kaksisuuntaisen kaapelitelevisioverkon päällä, ja yleisin toteutettu palvelu on internetyhteys. Kaapelimodeemilla savutetaan jopa 350 Mb/s sisäänpäin ja 20 Mb/s ulospäin, ja yhteysnopeus on yleensä asymmetrinen. (Wikipedia 2014c.)

Mobiililaajakaista voidaan toteuttaa esimerkiksi 3G- tai 4G-modeemilla, erillisellä nettitikulla tai päätelaitteessa, kuten kannettavassa tietokoneessa, olevalla sisäänrakennetulla mokkulalla. Langatonta tiedonsiirtoa käytettäessä tukiasemat hidastavat mobiilikaistan vauhtia, jos alueella on paljon puhelimen käyttäjiä. Mobiililaajakaistaa ei kannata valita ainoaksi nettiyhteydeksi, koska toimivuuteen vaikuttaa moni asia eivätkä operaattorit voi taata mitään tiettyä nopeutta liittymälle. (Wikipedia 2014b.)

3 WLAN

3.1 Standardit

Sähköteknisiä tieteitä edistävä IEEE on kansainvälinen organisaatio, joka valmistelee ja julkaisee standardeja. IEEE:llä ei ole virallista oikeutta julkaista maakohtaisia tai kansainvälisiä standardeja, joten viralliset standardointiorganisaatiot, kuten ISO (*International Standardization Organisation*), voivat ottaa käyttöön IEEE:n määritelmät. (Puska 2005, 26.)

IEEE:n lähi- ja alueverkkojen standardointia valmisteleva LMSG (*LAN/MAN Standardization Group*) on edistänyt lähiverkkolaitteitten yhteensopivuutta yli 20 vuoden ajan 802-standardilla. Myös WLAN-standardi 802.11 noudattaa tätä yleistä konseptia. (Puska 2005, 26–27.)

IEEE 802.11 -standardista (taulukko 2) käytetään myös nimitystä WLAN, ja yleiskielessä Wi-Fi, WLAN ja 802.11 tarkoittavat käytännössä samaa asiaa. IEEE:n standardoiman 802.11-verkon kovin kilpailija on Hiperlan, mutta 802.11 on tällä hetkellä markkinajohtaja Yhdysvalloissa ja Euroopassa. (Wikipedia 2014j.)

TAULUKKO 2. 802.11-standardit (Porras 2014)

Standardi	Taajuusalue	Modulointi	Signaalinopeus	Todellinen nopeus
802.11	2,4 GHz	FHSS ja DSSS	2 Mb/s	2 Mb/s
802.11a	5 GHz	OFDM	54 Mb/s	25 Mb/s
802.11b	2,4 GHz	DSSS	11 MB/s	6 Mb/s
802.11g	2,4 GHz	DSSS ja OFDM	54 Mb/s	25 Mb/s
802.11n	5 ja 2,4 GHz	OFDM	540 Mb/s	540 Mb/s
ETSI HiperLAN	5 GHz	OFDM	54 Mb/s	54 Mb/s

3.2 WLAN-verkon todentaminen ja salaus

Porttiperusteisessa verkkoonpääsymenetelmässä asiakkaan verkon käyttöä rajoitetaan langattoman verkon todennuspalvelimen ja loogisten porttien avulla. Langattomat laitteet toimivat loogisina portteina, joiden välille muodostuu päästä päähän -yhteyksiä. (Hakala & Vainio 2005, 170.)

Tavallisimmat käytössä olevat autentikointimenetelmät ovat WEP sekä 802.1x-standardiin pohjautuvat WPA ja WPA2. Menetelmistä 802.1x on kehittynein. Salausmenetelmistä suositeltavia ovat ainoastaan WPA2-AES ja WPA-TKIP, joita voidaan tarjota samassa verkossa (taulukko 3). Näistä WPA2-AES-salaus on suositeltavampi. (Funet 2014.)

TAULUKKO 3. Salausmenetelmät (Funet 2014)

	WPA	**WPA2**
TKIP	WPA-TKIP Hyvä salaus	WPA2-TKIP Harvoin käytetty
AES	WPA-AES Harvoin käytetty	WPA2-AES Paras salaus

WEP on perusmekanismi, joka perustuu tukiasemiin ja verkkokortteihin määriteltyihin salausavaimiin. Selausavainten avulla pystytään turvaamaan liikenteen luottamuksellisuus. Järjestelmä tukee useamman avaimen käyttöä, muttei automaattista avaimen vaihtoa. Tämä johtaa tilanteeseen, jossa käytetään koko ajan samaa avainta, mikä mahdollistaa salauksen murtamisen. WEP-liikenteen salausmenetelmä perustuu RC4-salausalgorytmiin, jota on arvosteltu heikkouksistaan. (Hakala & Vainio 2005, 168.)

WPA-salausprotokollan tarkoituksena on korjata WEP-protokollan puutteet. WPA-salausprotokolla vaihtaa salausavainta automaattisesti 10 000 paketin

jälkeen, ja järjestelmä käyttää pakettikohtaisia salausavaimia. WPA käyttää kahta protokollaa, joista TKIP hoitaa pakettien salauksen ja EAP mahdollistaa käyttäjien luotettavan tunnistuksen. Keskeisimmät heikkoudet ovat TKIP:n käyttäminen RC4-salauksessa ja protokollan reagointi palvelunestohyökkäyksiä kohtaan. (Hakala & Vainio 2005, 169.)

IEEE 802.11i eli WPA2 tarjoaa samat ratkaisut kuin aiempi WPA-standardi, mutta aiemman lisäksi WPA2 tarjoaa AES-salausmekanismin. AES on hyvin erilainen kuin WPA:n käyttämä RC4 ja pystyykin käyttämään eripituisia salausavaimia: 128-, 192- ja 256-bittisiä. AES:ää vastaan ei ole havaittu tehdyn yhtään tunnustettua palvelunestohyökkäystä, minkä vuoksi NSA on hyväksynyt AES-salausmekanismin turvaamaan NSA:n huippusalaisiksi luokitellut aineistot. (Wikipedia 2014j.)

Tietoturvaprotokollista TKIP sisältää avaimen säännöllisen uusimisen ja uuden avaimen luomisen jokaiselle kehykselle. AES-algoritmi taas tarjoaa kehyskohtaisen avaimen, ja siinä eheystarkistus on yhdistetty. AES-kryptaus tarjoaa erinomaisen tietoturvan, ja sitä suositellaan käytettäväksi kaikissa langattomissa verkoissa. Salausavainten TKIP:n ja AES:n pääavain luodaan salasanasta tai palvelimen avulla, ja sen on oltava tiedossa tukiasemalla ja päätelaitteella. Salausmenetelmistä PSK (*Pre Shared Key*) on menetelmä, jossa autentikointiin käytetään kaikille yhteistä avainta. PSK-salauksen käyttöä ei suositella, koska verkkoon päässyt käyttäjä näkee verkkoliikenteen salaamattomana. (Funet 2014.)

3.3 SSID ja WDS

SSID (*Service Set Identifier*) on langattoman verkon verkkotunnus. SSID:n avulla voidaan erottaa WLAN-verkot toisistaan ja liittyä haluttuun verkkoon. Korkeintaan 32-merkkinen verkkotunnus liitetään kaikkiin verkossa liikkuviin paketteihin ja sen avulla verkkojen liikenne voidaan erottaa toisistaan. SSID:n lähettäminen voidaan kytkeä pois, jolloin verkko ei näy kuuluvuusalueella. Tällä ei ole kuitenkaan merkitystä tietoturvan kannalta, koska uuden asiakkaan liittyessä

verkkoon SSID kulkee salaamattomana liittyjältä tukiasemaan (*Access Point*), jolloin SSID saadaan verkon kuuntelulla selville. (Wikipedia 2014j.)

WDS on langattomassa verkossa toimiva järjestelmä, joka mahdollistaa langattomasti WLAN-tukiasemien liittämisen toisiinsa. Tämä mahdollistaa verkon rakentamisen ilman fyysistä verkkokaapelia. WDS:n etu muihin langattomiin ratkaisuihin on kiinteän MAC-osoitteen säilyminen eri tukiasemien välillä. Tukiasemat käyttävät samaa radiokanavaa, ja yhteyden salaukseen voi valita WEP-, WPA- tai WPA2-salauksen. 802.11-standardi ei vielä määrittele WDS:ää, joten WDS-tukiasemien tulee olla samalta valmistajalta, jottei yhteensopimattomuusongelmia tule. (Wikipedia EN 2014.)

4 TIETOTURVA

4.1 Yleistä tietoturvasta

Tietoturvallisuus on tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista huijausyrityksiltä, roskapostilta, teollisuusvakoilulta, piratismilta ja tietokoneviruksilta. Tietoturvallisuuden uhkia voivat olla luvaton pääsy tietoihin, tiedon luvaton käyttö sekä tiedon kopioituminen tai häviäminen. (Wikipedia 2014g.) Tietoturvan kehittäminen on keskittynyt tietojen käsittelyyn ja perusturvallisuustason rakentamiseen (Luoti 2005).

Tietoturvallisuus voidaan jakaa kolmeen eri osa-alueeseen:

- luottamuksellisuus – tiedot eivät ole ulkopuolisten saavutettavissa, eikä niitä luovuteta tai paljasteta ulkopuolisille
- eheys – tietoihin ja järjestelmiin voidaan luottaa ja
- saatavuus – järjestelmien tiedot ovat tarvittaessa saatavilla (Luoti 2005).

Fyysinen tietoturva voidaan jakaa kolmeen osa-alueeseen: työasemat, palvelimet ja tietokoneverkko. Näistä työasemien tietoturvaan kuuluu käyttäjätunnusten ja käyttöoikeuksien hallinta. Tämän lisäksi palvelinympäristössä tulee tehdä varmuuskopiointia, auditoida järjestelmää ja asettaa verkon käyttörajoitukset. Verkon tietoturva koostuu fyysisistä ratkaisuista, kuten palomuurit, NAT-palvelut, kytkimet, reititys, verkonhallinta ja vianselvitys.

Tietoturvaa voidaan parantaa erilaisilla salausmenetelmillä, jolloin tieto on saatavilla vain avaimella tai tuntemalla salausmenetelmä. Myös sähköposteja voidaan salata. Silloin lukijan tulee tietää salausavain, mutta hän voi olla varma, että viesti todella on lähettäjältä.

Tietoturvasta huolehtimista varten on olemassa sekä kotimainen että kansainvälinen lainsäädäntö, joka asettaa suoria ja epäsuoria velvoitteita yrityksille. Velvoitteet ovat melko yleisluonteisia, ja niiden käytännön määrittely on jätetty yritysten vastuulle. Yritysten onkin keskeistä kartoittaa ne säädökset,

jotka koskevat niiden tietoturvan suunnittelua, ylläpitoa ja kehittämistä. (Laaksonen, Nevasalo & Tomula 2006, 18.)

Tietoturvan ei tulisi keskittyä vain ulkoa tuleviin uhkiin vaan huomioida myös sisäiset uhat. Työntekijän saastunut muistitikku voi aiheuttaa huonosti rakennetulle lähiverkolle massiivisia vaurioita, eikä tällöin ulkoa tulevien uhkien varalle rakennettu suojaus auta. Tietoturvaratkaisuissa tulisi muistaa eri puolilta tulevat uhat ja pyrkiä rakentamaan tietoverkko niin, että mahdollinen vaurio rajautuisi mahdollisimman harvaan koneeseen tai laitteeseen.

4.2 Langaton tietoturva

Viestisignaalit ovat tavoitettavissa avoimesti niiden edetessä. Sen vuoksi langatonta tietoverkkoa voi helposti tarkkailla, jos se on suojaamaton. Suojaamattoman verkon datapaketteja voidaan hakkerointityökalujen avulla seurata ja IP-pakettien salaamaton sisältö voidaan selvittää. Siksi langaton tietoverkko tuleekin suojata hyvin, esimerkiksi käyttämällä salausta, jossa salaisen avaimen avulla suojataan dataliikenne niin, ettei hakkeri pysty salausta purkamaan. (Geier 2005, 171–172.)

Hyvän tietoturvatason saavuttamiseksi on tärkeää määritellä tehokkaat käytännöt sekä niitä vastaavat toimeenpanoprosessit. Tietoturvan vaatimukset tulee määritellä hyvin, ja käyttöön on otettava tarvittava tietoturvataso. Salauksen tulisi olla osa langattoman verkon toteutusta, ja yrityksissä tulisi myös käyttää tehokkaimpia salausmenetelmiä. (Geier 2005, 190–191.)

4.3 Virustorjunta

Virustorjunta sisältää tietokoneohjelmia, jotka etsivät ja tuhoavat paikallisesta tai etäpisteestä haitallisia prosesseja, niiden tarvitsemia tiedostoja tai ajettavaan ohjelmistoon tarttuneita haittakoodeja. Virustorjunta pyrkii puhdistamaan työaseman sekä estämään viruksen leviämisen verkossa tai massamuistin välityksellä. Työtiedostoista kannattaa tehdä säännöllisesti varmuuskopioita, koska virukset voivat tehdä niistä käyttökelvottomia. (Wikipedia 2014h.)

Jos työntekijä käyttää etäyhteyttä yrityksen verkkoon, on syytä huomioida, että työntekijä käyttää tähän tarkoitukseen vain yritykseltä saamaansa tietokonetta. Tällöin voidaan varmistua siitä, että virustorjunta on ajanmukaisella tasolla. Työasemien virustorjunnan lisäksi tulee varmistaa, että palvelinympäristö, mobiililaitteet sekä internetliikenne ovat virustorjunnan piirissä. Selainliikenne voidaan esimerkiksi järjestää välityspalvelimen (*proxy*) kautta, jolloin palvelin hoitaa virusten torjunnan. Silti yrityksen toimintatavoilla ja henkilökunnan koulutuksella on merkitystä virusten torjunnassa. (Laaksonen ym. 2006, 204–205.)

Virustorjunnan osalta tulee tarkistaa ja varmistaa seuraavat asiat:

- työasemat
- etä- ja mobiililaitteet, mukaan lukien kotikoneet
- palvelimet
- tuotannollisten järjestelmät
- sähköposti-, selain- ja internetliikenne
- siirrettävät mediat, kuten USB-muistit ja iPod-soittimet
- tieturvavaatimukset
- sopimukset ja raportointikäytännöt ja seuranta
- toiminta virustapauksissa (Laaksonen ym.2006, 205).

4.4 Malwaret eli haittaohjelmat

Malware on yleisnimitys haittaohjelmille. Tunnetuin malwaretyyppi on tietokonevirus, mutta yleisiä malvareja ovat myös madot, troijanhevoset, RAT ja SPAM. (Boyle & Panko 2013, 18.)

Virukset ovat ohjelmia, joiden tarkoitus on hyökätä itseään vastaan, ja kärsijöinä ovat normaalit ohjelmat. Kun tartunta on saatu, lähettävät saastuneet ohjelmat

virusta muihin koneisiin. Aikaisemmin virukset siirtyivät korppujen kautta tietokoneesta toiseen, mutta nykyään virukset pystyvät siirtymään useammalla eri tavalla, kuten sähköpostiliitteiden, pikaviestimien ja tiedostonjako-ohjelmien välityksellä sekä internetsivuilta latausten yhteydessä. Virusten tekijät pyrkivät saastuttamaan yleisesti käytössä olevia ohjelmia, jotta aiheutuva haitta saadaan maksimoitua. (Boyle & Panko 2013, 18.)

Merkittävimmistä malwareista madot toimivat itsenäisesti, eli toisin kuin virukset, ne ovat itsenäisiä ohjelmia. Madot eivät siksi pyri hyökkäämään itseensä tai normaaleihin ohjelmiin. Ne pystyvät tarttumaan samoilla tavoilla kuin viruksetkin mutta ovat leviämisessään aggressiivisempia. Mato voi levitä ilman käyttäjän erityistä varomattomuutta, koska mato kykenee hyödyntämään erilaisia haavoittuvuuksia. (Boyle & Panko 2013, 20.)

Troijanhevonen on malware, joka piiloutuu normaaliksi ohjelmaksi. Troijanhevoset ovat levinneet ihmisten ladatessa piraattiohjelmia, jotka ovatkin osoittautuneet troijanhevosiksi. Piraattiohjelmia on vieläkin olemassa, mutta nykyään on tavallisempaa, että troijanhevonen kaappaa ja poistaa ohjelmistojärjestelmästä normaalin ohjelman tiedostonimen itselleen sekä käyttää normaalin ohjelman tiedostoja. Tämän vuoksi troijanhevosta on vaikea havaita. (Boyle & Panko 2013, 22–23.)

Remote Access Trojan eli RAT antaa hyökkääjälle etäyhteyden käyttäjän koneelle. Hyökkääjä voi tehdä isompaa tai pienempää haittaa käyttäjälle, kuten kirjoittamalla jotain näytölle tai avata CD-aseman. RAT-ohjelman voi saada lataamalla saastuneen etäkäyttöohjelman internetistä. (Boyle & Panko 2013, 23.)

SPAM eli roskaposti on ongelma, joka koskee kaikkia sähköpostin käyttäjiä. Roskapostin suodattimet ovat vähentäneet huomattavasti roskapostia, mutta siltikin ongelmia on edelleen. *Messagelabsin* tutkimuksen mukaan syyskuussa 2010 kaikesta liikenteestä 92 % oli roskapostia. Roskaposti voi mainostaa jotain tai se voi sisältää viruksen, madon, troijanhevosen tai muita haittaohjelmia. (Boyle & Panko 2013, 26.)

4.5 Palomuuri ja NAT (*Network Address Translation*)

Palomuuri voi olla laite tai ohjelma, joka rajoittaa sekä valvoo tietokoneen ja ulkoverkon välistä liikennettä. Palomuurilla pyritään estämään verkon kautta tapahtuva luvaton ja näkymätön käyttö. Palomuuri ehkäisee myös mahdollisten virusten yhteyttä ulkoverkkoon. (Korpela 2005, 86.)

Kaikki IP-paketit kulkevat palomuurin läpi. Jos paketti todetaan uhkaavaksi tai se ei ole sallittu, hylkää palomuuri sen läpi pääsyn, ja jos pakettia ei todeta uhkaavaksi tai kielletyksi, paketti pääsee lävitse. Myös uhkaavat paketit, joita palomuuri ei tunnista, pääsevät läpi. Palomuuri pitää kirjaa niistä paketeista, joita se ei päästänyt lävitse. Sen vuoksi ylläpitäjän onkin hyvä seurata lokia päivittäin tai jopa useammin, koska lokista voidaan saada tärkeää tietoa uhkaavista paketeista ja siitä, mistä vahingollista liikennettä tulee. Järjestelmän ylläpitäjä voi tarvittaessa sulkea IP-osoitteen, josta haitallista liikennettä tulee jatkuvasti. (Boyle & Panko 2013, 351.)

NAT on IP-osoitteiden konvertoija, joka toimii reitittimessä. NAT mahdollistaa sisäverkon osoitteiden näkymättömyyden käyttämällä eri IP-osoitteita sisä- ja ulkoverkossa. NAT suojaa sisäverkkoa ohjaamalla sisäverkon verkkoliikenteen ulkoverkkoon päin yhden IP-osoitteen taakse. Tällä säästetään IP-osoitteita, koska yhden ulkoisen IP-osoitteen takana voi olla useita tietokoneita. Myös tietoturva paranee, koska näin sisäverkon rakenne ei näy ulospäin. (Cisco 2013.)

5 VPN (*Virtual Private Network*)

VPN-verkon tarkoituksena on luoda kahden pisteen välille turvallinen datayhteys hyödyntämällä julkisia verkkoja, kuten internetiä. VPN-määritelmää käytetään myös yksittäisten etätyöasemien liittämisestä yksityisverkkoon. (Wikipedia 2014i.)

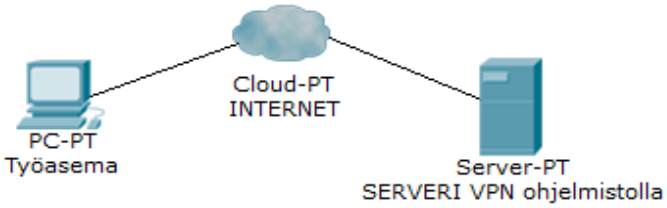
VPN-verkossa yhteysosapuolten välille muodostetaan virtuaalinen tunneli, jonka avulla voidaan siirtää dataa julkisen verkon yli. Nykyään pelkän tunnelin luominen ei riitä, vaan myös tietoturva-asiat on otettava huomioon, mikä edellyttää siirrettävän datan salausta ja käyttäjien tunnistamista. Yhteyden muodostamisessa yrityksen kahden toimipisteen välille käytetään molemmissa päissä sopivia reitittimiä. Yhden käyttäjän etäyhteys puolestaan muodostetaan suoraan etäkäyttöpalvelimelle erillisen VPN-ohjelmiston avulla. (Hakala & Vainio 2005, 381–382.)

VPN-yhteydet voidaan jakaa kolmeen eri luokkaan: Host-to-Host VPN, Remote Access VPN ja Site-to-Site VPN. Kaikissa VPN-yhteyksissä tieto salataan ennen sen liikkumista julkisen verkon eli esimerkiksi internetin kautta. Maailmanlaajuisesti Host-to-Host ja Remote Access VPN -yhteyksissä käytetään salausmenetelmänä SSL/TLS-standardia. Site-to-Site VPN -yhteys ei käytä ohjelmallista SSL/TLS-salausohjelmaa, vaan VPN-yhteyden salaus hoidetaan esimerkiksi ADSL-päätelaitteessa, ja siksi Site-to-Site -yhteyden avulla saavutetaan huomattavasti suurempi tiedonsiirtokapasiteetti. (Boyle & Panko 2013, 171–179.)

5.1 VPN:n yhteystavat

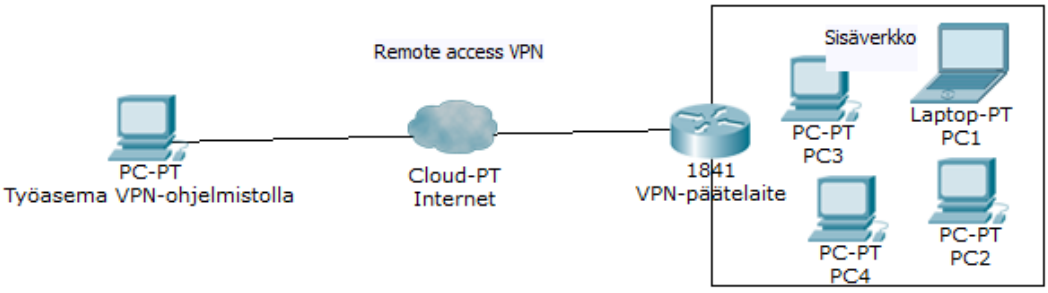
Host-to-Host -yhteydessä (kuvio 2) pystytään yhdistämään yksi käyttäjä internetin välityksellä serverille VPN-tunnelia käyttämällä. Host-to-Host VPN -yhteyttä käytetään yleensä verkkokaupoissa, kun on tarvetta käyttää suojattua yhteyttä,

esimerkiksi luottokorttitietoja annettaessa. (Boyle & Panko 2013, 172.)



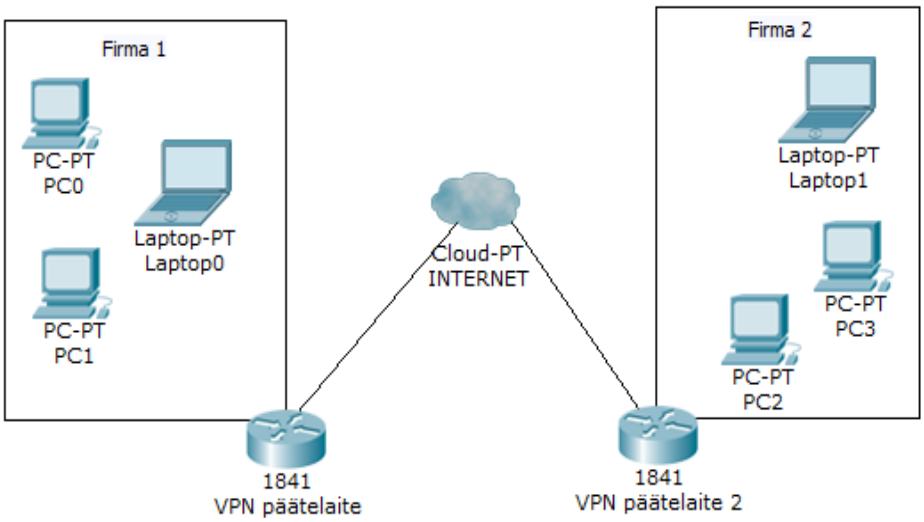
KUVIO 2. Host-to-Host VPN

Remote Access VPN -yhteydessä (kuvio 3) muodostetaan yhden tietokoneen ja yksityisen verkon välille suojattu yhteys. Remote Access VPN -yhteys palvelee työntekijöitä, joilla on työnsä luonteen vuoksi tarve käyttää tietokonetta ja saada yhteys yrityksen tietoverkkoon myös kotona ja matkoilla. Tarvittaessa VPN-yhteys voi tarjota suojatun yhteyden yrityksen ja yhteistyökumppanien välille. (Boyle & Panko 2013, 172.)



KUVIO 3. Remote Access VPN

Site-to-Site VPN -yhteys (kuvio 4) tarjoaa suojan kaikenlaiselle internetin kautta kulkevalle verkkoliikenteelle yhdistettäessä kaksi yksityisverkkoa toisiinsa. Site-to-Site VPN -yhteydellä voidaan jakaa yrityksen oma lähiverkko kahden toimipisteen välillä tai VPN-yhteys kahden erillisen yksityisverkon välillä. (Boyle & Panko 2013, 173.)



KUVIO 4. Site-to-Site VPN

5.2 VPN-prototokollat

VPN-yhteyksissä voidaan salaukseen käyttää erilaisia tunnelointiprotokollia, joista julkisesti on standardoitu IPsec, L2TP, L2F, L2TP ja PPTP. Lähiverkkojen yhdistämiseen ja etäkäyttöön sopii IPsec ESP-tunnelointimoodissa. Pelkästään lähiverkkojen yhdistämiseen sopii L2F ja pelkästään etäkäyttöön L2TP ja PPTP. SSL VPN poikkeaa muista protokollista, koska se muodostaa salatun yhteyden yrityksen tietojärjestelmään mutta estää silti IP-pakettiliikenteen pääsyn yrityksen tietoverkkoon. (Wikipedia 2014i.)

Tunnelointiprotokolla IPsec sisältää joukon TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia, jotka on tarkoitettu internetyhteyksien turvaamiseksi. IPsec määrittelee protokollat pakettivirtojen turvaamiseksi ja avaintenvaihtoprotokollat turvattujen pakettivirtojen muodostamiseen. Tietoliikenneprotokollat tarjoavat salauksen, osapuolten todennuksen ja tiedon eheyden varmistuksen. IPseciä voidaan hyödyntää VPN-ratkaisuissa, koska se toimii OSI-mallin kolmannella tasolla ja on näin joustavampi kuin ylemmällä tasolla toimivat protokollat. (Wikipedia 2014i.)

IPsecin eniten käyttämät protokollat ovat pakettivirtojen turvaamisprotokollat AH ja ESP sekä avaintenvaihtoprotokolla IKE. Näistä AH ei pysty salaamaan paketteja, mutta mahdollistaa eheyden ja todentamisen pakettien otsikoille sekä datalle. Ennen IPsecin versiota 2 käytettiin AH:ta ja ESP:tä yhdessä, mutta IPsecin versio 2 mahdollisti ESP:lle kyvyn autentikoida paketteja. Tästä syystä AH-protokollan käyttö on nykyisin vähäistä, mutta sillä pystytään edelleen autentikoimaan sellaisia paketin osia, joita EPS ei pysty autentikoimaan. (Frankel, Kent, Lewkowski, Orebaugh, Ritchey & Sahrma 2005, 3-1.)

ESP voi toimia tunneli- tai kuljetustilassa, joista tunnelitila on käytetetympi. Tunnelitilassa ESP pystyy salaamaan niin datan kuin IP-paketin otsikon. Tällöin väärinkäytösten mahdollisuus on pieni, koska datan salauksen lisäksi IP-otsikoiden salaaminen peittää lähettäjän ja vastaanottajan tiedot. ESP:n kuljetuskäytössä alkuperäinen IP-otsikko säilyy, mutta data on salattua. IP-otsikon säilymisen vuoksi kuljetuskäyttö ei ole niin turvallinen, eikä sitä käytetä yleensä muuten kuin Host-to-Host -yhteyksissä. IPsec-pakettien kanssa ESP käyttää symmetristä salausta, jossa molempien päitten on käytettävä samaa avainta pakettien purkamiseen ja salaamiseen. (Frankel ym. 2005, 3-5 – 3-6.)

SSL VPN -yhteydessä VPN-yhteys ottaa tunnelin SSL-yhteyden välityksellä, jolloin molempia hyödyntäen päästään esimerkiksi etätyöasemalta suljettuun verkkoon. SSL VPN toimii OSI-mallin ylemmillä kerroksilla, ja sen ei tarvitse huolehtia tiedonsiirron luotettavuudesta. SSL VPN:ää ei ole standardoitu, ja siksi kaikki päätelaitteet eivät tue sitä. (Wikipedia 2014f.)

PPTP on VPN-tunnelointiprotokolla, joka pohjautuu PPP-kehysten tunnelointiin TCP/IP-verkon läpi. Data salataan ennen PPP-kehyksen kapselointia käyttäjän salausavainten avulla, minkä jälkeen käyttäjän tunnistukseen käytetään PAP:ta, CHAP:ta tai EAP:ta (Hakala 2005, 382–383). PPTP-protokollaa on käytetty Windows-työasemien kytkemiseen Windows-palvelimeen julkisen verkon kautta (Wikipedia 2014i).

L2TP on moniprotokollaratkaisu, joka on yhdistelmä PPTP- ja L2F-protokollista. Toisin kuin PPTP-protokollassa, ei L2TP salaa MPPE:llä PPP-kehyksiä. L2TP luottaa IPsecin kuljetustilan salausmenetelmiin, ja L2TP:n ja IPsecin kombinaatiota kutsutaan nimellä L2TP/IPsec. (Windows Server 2008.)

GRE on IP-tunnelointiprotokolla, jonka CISCO on kehittänyt. GRE:n sisällä tunneloidaan yleensä VPN-yhteyksiä sekä IP-paketteja. Protokollan tuki on monissa laitteissa keskeneräinen, mutta itsessään GRE:ssä on hyvä hyötysuhde. Protokollan tuen keskeneräisyyden vuoksi GRE:tä käyttävät VPN-yhteydet saattavat toisinaan toimia hyvin ennalta arvaamattomasti. (Wikipedia 2014a.)

6 TIETOVERKON LAAJENNUS

6.1 Lähtötilanne

TMT. Malinen Oy:n toimipisteistä vain keskustoimistolla on suora lähiverkkoyhteys käytössään. Tytäryhtiöissä yhteydet lähiverkkoon ja sen kautta tuotannonohjausjärjestelmään on toteutettu työasemakohtaisilla VPN-ohjelmistoilla. Opinnäytetyön tarkoituksena on tehdä selvitys, mitä mahdollisuuksia olisi laajentaa VPN-yhteyden avulla lähiverkko toimimaan yhtiön muissa toimipisteissä. VPN-yhteyden lisäksi työssä selvitetään lähiverkon laajentamista tytäryhtiön sisällä.

Lähiverkon laajentaminen on tarkoitus aloittaa TMT. Malinen Oy:n tytäryhtiön Vuoripoika Oy:n tuotanto- ja toimistotiloista. Tulevaisuudessa tuotannonohjausjärjestelmän laajentaminen myös tuotantotyöntekijöiden käyttöön voi olla ajankohtaista, ja siksi lähiverkko suunnitellaan kattamaan toimisto- ja tuotantotilat 1 ja 2 (kuvio 5).

KUVIO 5. Vuoripoika Oy:n toimisto ja tuotantotilat (Google 2014)

Suunnitellun laajennusratkaisun tulisi olla tarvittaessa siirrettävä sekä helposti monistettavissa. Tulevan ratkaisun tulisi olla myös edullinen. Siksi työssä päädyttiin käsittelemään langattomia järjestelmiä, joissa kustannuksia nostavat sekä siirrettävyyttä hankaloittavat pitkät kaapeloinnit on jätetty pois.

KUVIO 6. Tämänhetkinen verkkoratkaisu (Google 2014)

Tällä hetkellä tuotantotila 1:ssä olevaan huoneeseen on sijoitettu CISCO 887VAE ADSL/VDSL -modeemi ja sen perään on kytketty WLAN-tukiasema TP-LINK (kuvio 6). Tietokoneen ja laajakaistayhteyden käyttö on suurinta toimistotiloissa, joissa WLAN-signaali toimii huomattavan vaimentuneesti. WLAN-tukiasema kattaa kohtuullisesti tuotantotila yhden ja toimiston, mutta tuotantotila kahdessa WLAN-yhteyttä ei pystytä muodostamaan.

6.2 Tietoverkon kartoitus

Tällä hetkellä Vuoripoika Oy:ssä on langaton internetyhteys ADSL-modeemilla ja toimistossa kannettava tietokone, joka ottaa ohjelmallisen VPN-yhteyden kautta yhteyden TMT. Malinen Oy:n lähiverkkoon. Tuotantotila yhden (kuvio 9) puolivälissä olevan ADSL-modeemin WLAN:n kantavuus riittää tyydyttävästi toimistotiloihin.

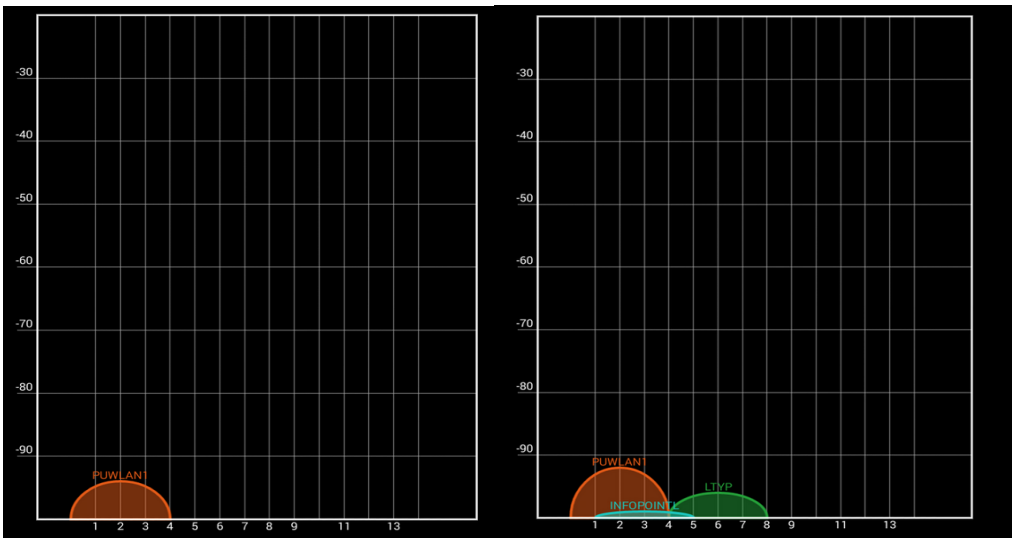
Vuoripoika Oy:n ADSL-modeemi on operaattorilta vuokrattu CISCO 887VAE, jolla voitaisiin myös tarvittaessa muodostaa Site-to-Site VPN -yhteys yhtiön toimipisteiden välille. Puhelinverkon pistorasioita on myös toimistotiloissa, joten tulevaisuudessa ADSL-modeemi voi sijaita myös siellä.

6.3 WLAN-verkkojen kartoitus

Suunnitellun langattoman verkon optimoimiseksi Vuoripoika Oy:n tiloissa tehtiin olemassa olevien WLAN-verkkojen sekä niiden käyttämien kanavien kartoitus. Kartoitus toteutettiin Samsung Galaxy S5 -miniälypuhelimella ja siihen hankitulla applikaatiolla, joka tunnistaa näkyvät WLAN-verkot. Applikaatio tunnistaa 2,4:n ja 5 gigahertsin WLAN-verkot sekä verkkojen käyttämät kanavat.

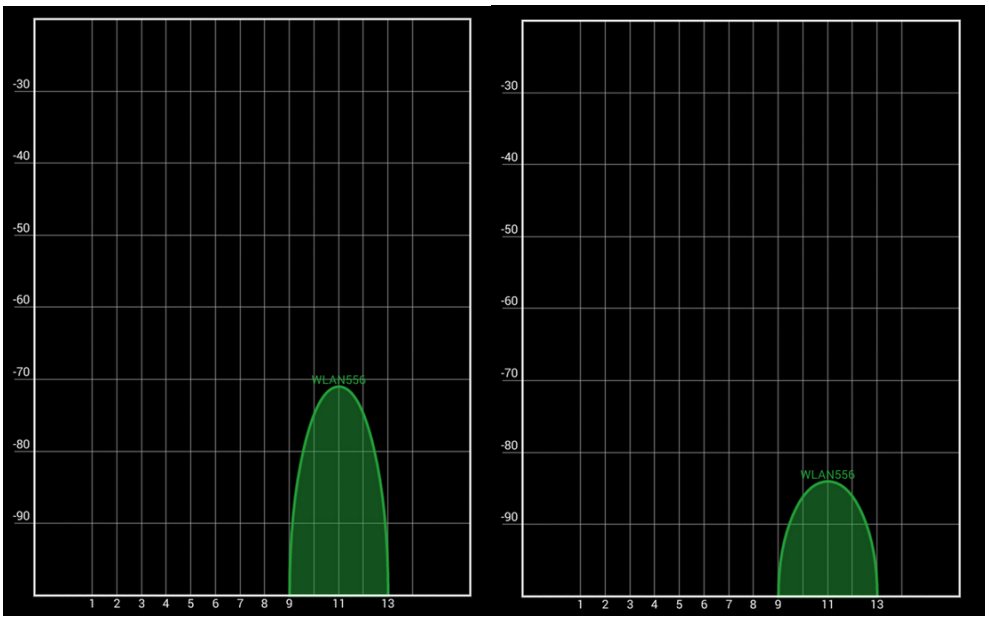
Mittaukset aloitettiin tuotantotila kahdesta (kuvio 7:n sijainnit 1 ja 2). Kuviossa 8 nähdään mittaustulokset, jotka osoittavat kolmen WLAN-verkon kantavan tuotantotiloihin. Verkkojen voimakkuudet olivat heikkoja, ja niiden vaikutus on vähäinen langattoman verkon suunnittelussa.

KUVIO 7. Mittauspaikat (Google 2014)



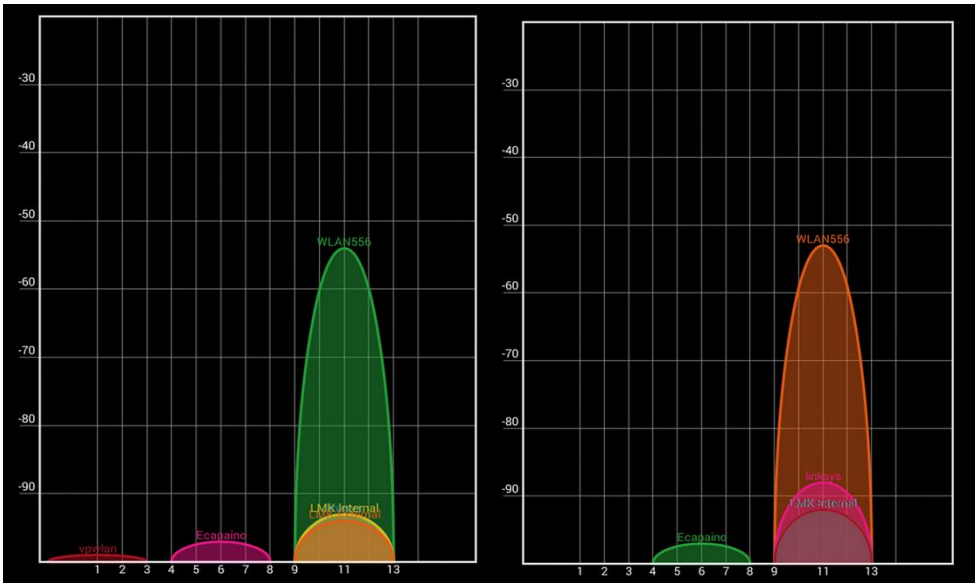
KUVIO 8. Tuotantotila 2:ssa havaitut WLAN-verkot. Sijainti 1 vasemmalla ja sijainti 2 oikealla (Wifi Analyzer 2014)

Mittauksia jatkettiin tuotantila yhteen, kuvion 7 sijainteihin 3 ja 4. Mittaustuloksista voidaan todeta, että tuotantila yhden pohjois- ja itäosaan kantaa vain Vuoripoika Oy:n oma WLAN-verkko (SSID: WLAN556) (kuvio 9). Tuotantotila 1:n itäosaan WLAN-verkko kantaa huonosti tai kohtuullisesti, ja kantamaa rajoittaa tiilirakenteinen väliseinä.



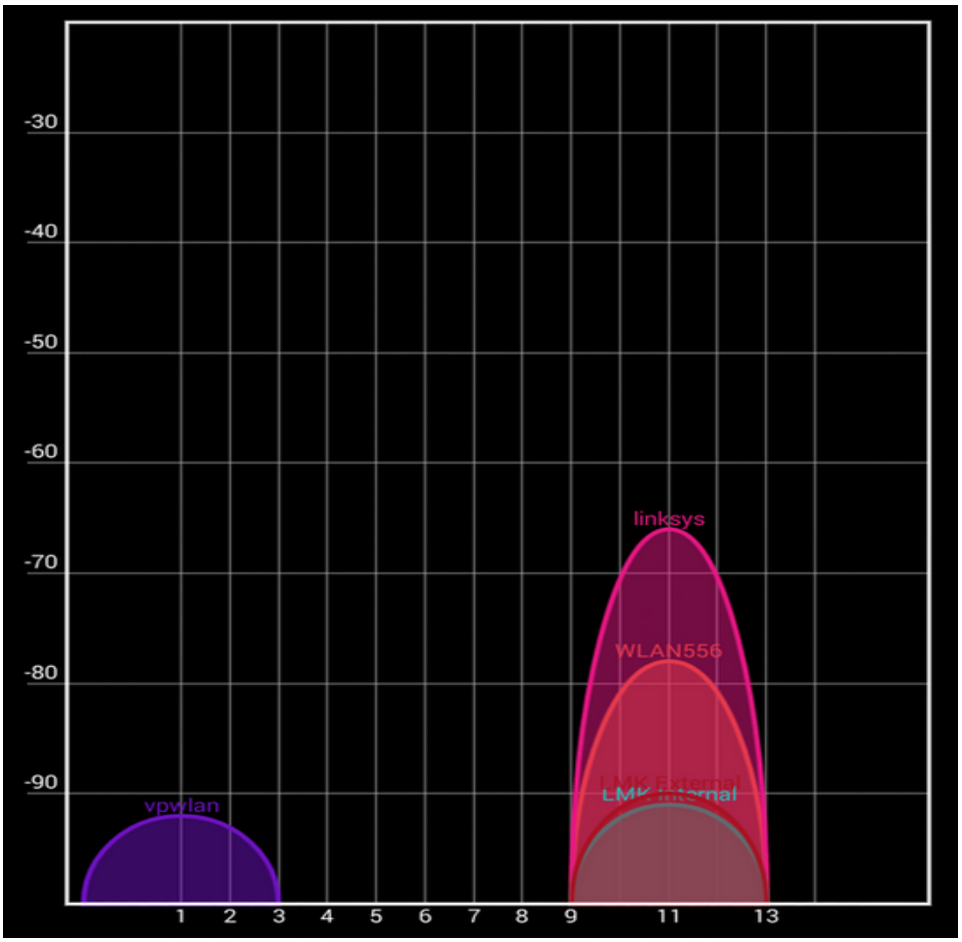
KUVIO 9. Tuotantila 1:n WLAN-verkot, sijainti 3 vasemmalla ja sijainti 4 oikealla (Wifi Analyzer 2014)

Tuotantotila 1:n keskellä (kuvio 7, sijainti 5) WLAN-verkkoja havaitaan kuusi kappaletta (kuvio 10). Vahvimpana verkkona on Vuoripoika Oy:n oma WLAN-verkko, mutta samalla WLAN-kanavalla havaitaan kolme muutakin verkkoa. Samalla kanavalla olevat WLAN-verkot hidastavat Vuoripoika Oy:n langatonta verkkoa, jos kaikkia verkkoja käytetään yhtäaikaisesti.



KUVIO 10. Tuotantotila 1:n ja toimistotilan WLAN-verkot, sijainti 5 vasemmalla ja sijainti 6 oikealla (Wifi Analyzer 2014)

Vuoripoika Oy:n langaton verkko toimii kohtuullisesti toimistotiloihin asti (kuvio 7, sijainti 6). Kuitenkin suljettaessa toimiston ovi havaitaan WLAN-verkon voimakkuudessa huomattava lasku (kuviot 10 ja 11), joka vaikuttaa tiedonsiirtonopeuteen. Mittaukset osoittavat, että toimiston oven sulkemisen jälkeen naapuriyrityksen käyttämä WLAN-verkon signaali on voimakkaampi kuin Vuoripoika Oy:n WLAN-verkko. Kuten tuotantila 1:ssä (kuvio 7, sijainti 5) huomattiin, on samalla WLAN-kanavalla myös toimiston alueella havaittavissa neljä ulkopuolista WLAN-verkkoa.



KUVIO 11. Toimistotilan WLAN-verkot, sijainti 6, toimiston ovi tuotantotila 1:een suljettuna (Wifi Analyzer 2014)

Suoritettujen mittausten perusteella nähdään, että WLAN-kanavista suurimmalla käytöllä oli WLAN-kanava 11, jolla Vuoripoika Oy:n omakin WLAN-verkko on. Kanavilla 4, 5, 7, 8, 9, 10, 12 ja 13 ei mittauksissa havaittu liikettä, joten yhtä

näistä suositellaan verkolle WLAN-kanavaksi. Mittaukset osoittavat, että toimiston tiedonsiirtonopeutta tulee kasvattaa parantamalla langatonta verkkoa tai tuomalla toimistotilaan kiinteä kaapeliyhteys.

6.4 Uudistusta tarvitsevat osa-alueet

Lähtökohtana Vuoripoika Oy:n tiloihin tulevalle lähiverkolle on saada toimiva Site-to-Site VPN-yhteys TMT. Malinen Oy:n lähiverkkoon. Tästä syystä tulevan päätelaitteen tulee tukea IPsec VPN -tunnelointia, jottei seurauksena ole yhteensopimattomuusongelmia.

Vuoripoika Oy:n tiloissa oleva internetyhteys on toteutettu CISCO 887VAE -modeemilla sekä TP-LINK WLAN -tukiasemalla, ja riippuen kokoonpanosta on näitä myös mahdollisuus hyödyntää. Vertailutaulukossa esitetyt palomuurilaitteet (Zyxel Zywall USG 20 W ja D-link DSR-1000N) tarvitsevat olemassa olevan ADSL-modeemin tai internetyhteyden, koska niissä ei ole modeemin ominaisuuksia. Vaihtoehtoisesti valitaan uusi modeemi, jonka ominaisuuksiin kuuluu sisäänrakennettu VPN-tunnelointi.

Koska tuotantotilat ovat suhteellisen laajat, tulee WLAN-tukiasemia sijoittaa tilaan vähintään neljä kappaletta. Neljällä tukiasemalla saavutetaan riittävä langattoman verkon peitto sekä tuotanto- että toimistotiloihin, ja näin työasemien sijoittelu on tulevaisuudessa vapaata. WLAN-tukiasemina käytettäisiin WDS-tuen omaavia tukiasemia, joiden liitettävyys keskenään ei vaadi kiinteää kaapelointia. Näistä WLAN-tukiasemista voidaan tarvittaessa tuoda ethernetkaapeli laitteille, jotka eivät WLAN-yhteyttä tue. WLAN-tukiasemien tulee olla samalta valmistajalta, jotta yhteensopimattomuusongelmilta vältytään.

6.5 Siirrettävyys ja monistettavuus

Verkon suunnittelun yhtenä lähtökohtana oli sen helppo siirrettävyys sekä monistettavuus yhtiön muihin tuotanto- ja toimistotiloihin. Koska toimipisteet eivät ole kovin suuria eivätkä työasemien määrä tai dataliikenteen käyttö kovin

suurta, keskityttiin edullisten ja yksinkertaisten mutta luotettavien laitteitten vertailuun.

Laitesuosituksissa on lähdetty siitä, että suositellut kokoonpanot toimivat kokonaisratkaisuina. Vaihtoehtoisesti kokoonpano sisältää ADSL-modeemin tai se toimii olemassa olevan internetyhteyden päällä palomuuripäätelaitteella.

6.6 Ratkaisumalleja tulevalle verkolle

Lähtökohtana tulevalle tietoverkon uudistukselle oli VPN-yhteyden rakentaminen ja sen jakaminen langattomasti WLAN-yhteyden avulla Vuoripoika Oy:n tiloissa. Laitevalmistajat tarjoavat paljon erilaisia ratkaisuja toteuttaa lähiverkko VPN-yhteydellä, mutta koska suunnittelussa rajoina olivat hinta, monistettavuus sekä siirrettävyys, käsitellään tässä työssä edullisia mutta tehokkaita laitteita.

Laitevalmistajien erilaisista vaihtoehdoista on otettu tähän työhön edullisimmat ja tehokkaimmat mallit (taulukot 5 ja 6). Alun perin suunnitellun ADSL/VDSL-modeemin, VPN-yhteyden sekä WDS-tuen omaavaa päätelaitetta ei tällä hetkellä löydy isoimmilta laitevalmistajilta. Siksi vertailuun päädyttiinkin ottamaan kaksi ADSL/VDSL-modeemia (Zyxel SBG3300-N ja Cisco 867VAE), joissa on tarvittavat VPN-tunnelointiominaisuudet. Toisena parina vertailuun otettiin kaksi palomuuripäätelaitetta (Zyxel Zywall USG 20 W ja D-link DSR-1000N), joissa on VPN-tunnelointimahdollisuudet sekä WDS-tuki.

WLAN-tukiasemiksi valikoituivat Zyxel WAP 3205 ja D-link DIR-615 (kuvio 17), joiden valinta riippuu palomuuripäätelaitteen valinnasta. WLAN-tukiasema sekä palomuuripäätelaitteet tulee valita samalta toimittajalta, jotta WDS:n yhteensopivuusongelmilta vältytään. Valittaessa uusi ADSL/VDSL-modeemi voidaan valita WLAN-tukiasemiksi kumpikin vaihtoehto, koska ensimmäinen WLAN-tukiasema tulee kiinnittää fyysisellä kaapelilla modeemiin.

TAULUKKO 5. Päätelaitteitten vertailutaulukko 1

Laite	Zyxel SBG3300-N	Zyxel ZyWall USG 20 W	Cisco 867VAE	D-Link DSR-1000N
Hinta	149,90 €	231,90 €	351,90 €	398,90 €
Modeemi	X	-	X	-
ADSL	X	-	X	-
ADSL2	X	-	X	-
VDSL2	X	-	X	-
WLAN	X	X	-	X
Ethernet	4 kpl	4 kpl	4 kpl	4 kpl
WDS	-	X	-	X

TAULUKKO 6. Päätelaitteitten vertailutaulukko 2

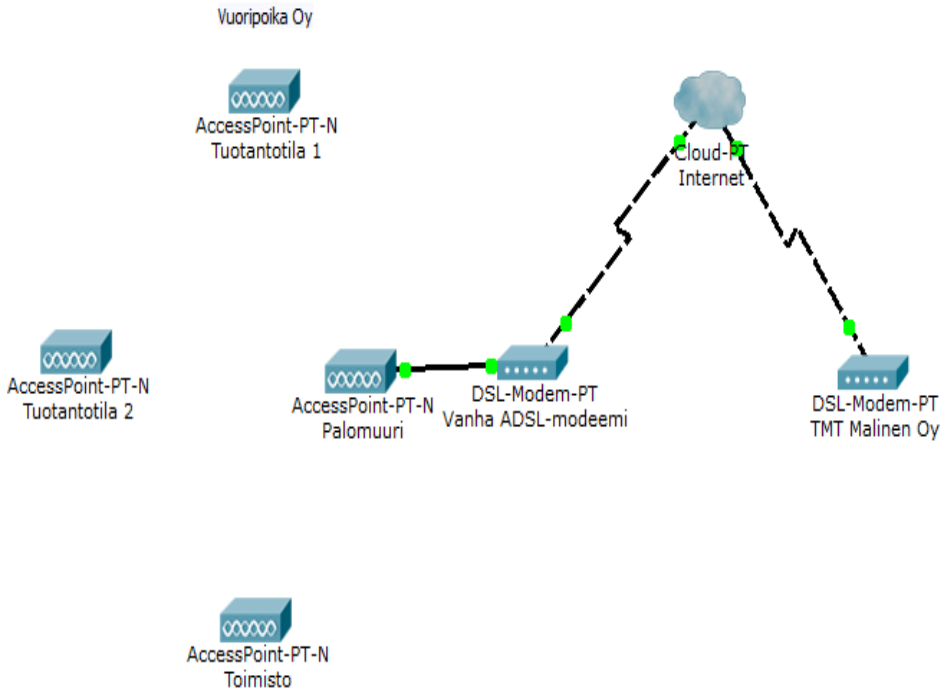
Laite	Zyxel SBG3300-N	Zyxel ZyWall USG 20 W	Cisco 867VAE	D-Link DSR-1000N
Hinta	149,90 €	231,90 €	351,90 €	398,90 €
VPN				
IPsec	X	X	X	X
PPTP	X	-	X	X
L2TP	X	-	X	X
SSL VPN	-	X	-	-
TUNNELIT				
SSL VPN	-	1 kpl	-	20 kpl
IPsec	20 kpl	5 kpl	10 kpl	70 kpl

TAULUKKO 7. WLAN-päätelaitteitten vertailutaulukko

Laite	Zyxel WAP3205	D-Link DIR-615
Hinta	39,90 €	30,90 €
WDS	X	X
WLAN:n nopeus Mbps	300	300
Ethernet	2 kpl	4 kpl

Tietoverkon uudistus suositellaan tehtäväksi jommallakummalla alla esitetyllä tavalla:

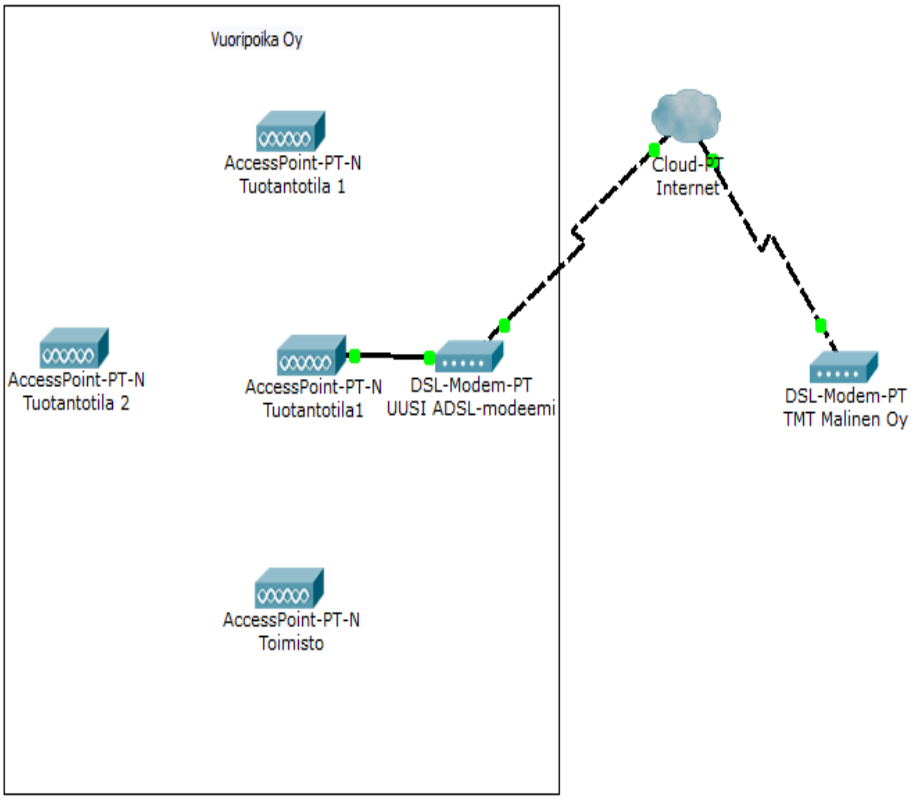
- Vaihtoehto 1 (kuvio 12): Ensimmäisessä vaihtoehdossa käytetään vanhaa internetyhteyttä ja ADSL-modeemia, johon liitetään Zyxel Zywall USG 20 W- tai D-link DSR-1000N -palomuuripäätelaite ethernetkaapelin avulla (kuvio 12). Palomuuripäätelaitteeseen liitetään kolme kappaletta WLAN-tukiasemia langattomasti WDS-yhteydellä. WLAN-tukiasemat liitetään myös keskenään langattomasti WDS-yhteyden avulla.



KUVIO 12. Lähiverkon uudistus, vaihtoehto 1

- Vaihtoehto 2 (kuvio 13): ADSL-modeemi vaihdetaan VPN-tunnelia tukevaksi ja VPN-yhteys muodostetaan uudella modeemilla. Modeemin ja yhden WLAN-tukiaseman välille kytketään ethernetkaapeli, ja tästä WLAN-tukiasemasta eteenpäin WLAN-yhteys jaetaan neljän WLAN-

tukiasemien välityksellä ja WDS-yhteyden avulla Vuoripoika Oy:n tiloissa.



KUVIO 13. Lähiverkon uudistus, vaihtoehto 2

Ensimmäisessä vaihtoehdossa käytetään vanhaa modeemia, jonka perään asennetaan palomuuripäätelaite ja WLAN-tukiasemat.Vertailtaessa D-link DSR-1000N:n ja Zyxel Zywall USG 20 W:n ominaisuuksia suurin ero oli VPN-yhteyksien tunnelointimäärissä, ja näistä D-link oli selkeästi tehokkaampi. VPN-yhteyksiä ei kuitenkaan tarvita useita, joten edullisempi ja muuten riittävillä ominaisuuksilla varustettu Zyxel on järkevä vaihtoehto. Zyxel-palomuuripäätelaite ja kolme kappaletta Zyxel WLAN-tukiasemia maksavat yhteensä 351,60 euroa (Verkkokauppa.com 2014).

Toinen ratkaisumalli voidaan toteuttaa Zyxelin SBG-3300-N- tai Ciscon 867VAE ADSL/VDSL -modeemin ja neljän WLAN-tukiaseman avulla. Cisco on monipuolisempi ja markkinoilla tunnetumpi toimija, mutta myös Zyxel on luotettava valmistaja. Eroja ominaisuuksissa on jonkin verran, mutta vertailtavista

ominaisuuksista suurin ero on yhtäaikaisten SSL VPN -yhteyksien määrässä, joita Zyxelissä on vain yksi. SSL VPN -ominaisuutta tarvittaisiin, jos Remote Access VPN -yhteys tai Host-to-Host VPN -yhteys muodostettaisiin Vuoripoika Oy:hyn. Mutta koska tarkoituksena on ottaa Site-to-Site VPN -yhteys Vuoripoika Oy:stä TMT. Malinen Oy:hyn, käy Zyxel suunniteltuun tarkoitukseen. Laitteitten välillä on huomattava hintaero eikä selkeää hyötyä kalliimmasta Ciscon modeemista tässä käyttötarkoituksessa saavuteta. Siksi suositellaan valittavaksi Zyxel SBG3300-N ja neljä kappaletta Zyxel WAP3205 WLAN -tukiasemia yhteishintaan 309,50 euroa (Verkkokauppa.com 2014).

Ottaen huomioon tilaajan toivomukset tietoverkkoratkaisun monistettavuudesta ja siirrettävyydestä suositellaan tietoverkon uudistamiseen valittavaksi Zyxel Zywall USG 20 W -palomuuripäätelaite sekä kolme kappaletta Zyxel WAP3205 WLAN -tukiasemia (kuvio 14). Ratkaisussa vanha ADSL-modeemi säilyttettäisiin, samoin tarvittaessa myös vanha WLAN-tukiasema. Jos vanha WLAN-tukiasema säilytetään, voidaan käyttää uuden lähiverkon rinnalla myös suoraa internetyhteyttä kuten ennenkin. Vanhaa internetyhteyttä voitaisiin hyödyntää tarvittaessa, esimerkiksi jos VPN-yhteydessä tai TMT. Malinen Oy:n verkkoyhteydessä olisi vikaa. Karkea suunnitelma uudelle lähiverkolle esitetään kuviossa 15.

KUVIO 14. Zyxel Zywall USG 20 W (vasemmalla) ja Zyxel WAP3205 (Verkkokauppa 2014)

Valittaessa vaihtoehto kaksi ei ADSL-modeemia tarvitse siirtää tämänhetkisestä sijainnistaan tuotantotila ykkösestä, mutta sen siirtäminen toimistoon voisi olla järkevää. Jos ADSL-modeemi siirretään, saataisiin toimiston tietokoneet sekä tulostimet tarvittaessa kiinteästi ethernetkaapelin päähän. Vaikka tietoverkon uudistus toteutettaisiinkin heti ilman ADSL-modeemin siirtoa, on vanhan ADSL-modeemin siirto helppoa myöhemmin, koska uusi tietoverkko on hyvin skaalautuva ja laitteitten sijoittelua on helppo muuttaa tarvittaessa.

KUVIO 15. Karkea suunnitelma päätelaitteitten sijoittelusta (Google 2014)

6.7 IP-päätelaitteet

Tietoverkon uudistuksen yhteydessä kaikki työasemat ja tulostimet voidaan liittää lähiverkkoon, ensisijaisesti langattomasti, mutta tarvittaessa myös ethernetkaapelilla. Lähiverkossa voidaan tarvittaessa muodostaa etäyhteys toiseen työasemaan ja muutoksia asetuksiin voidaan tehdä toimipisteitten välillä. Myös

keskitetyt päivitykset tietokoneille on helpompi järjestää, kun käytössä on yhteinen lähiverkko.

Tilaajan toivomusten mukaisesti myös tulostimet voidaan lisätä lähiverkkoon kummassakin toimipisteessä. Tulostimien lisääminen mahdollistaa tulostamisen kaikilta koneilta mihin tulostimeen tahansa, ja tarvittaessa paikallisista tulostimista voidaan siirtyä toimipistekohtaisiin verkkotulostimiin.

6.8 Tietoverkon uudistussuunnitelma

Tarkoituksena on aikaansaada edullinen, hyvin monistettava ja tarvittaessa helposti siirrettävä tietoverkkoratkaisu, jonka avulla saadaan laajennettua TMT. Malinen Oy:n lähiverkko toimimaan TMT. Malinen Oy:n tytäryhtiössä ja ensisijaisesti työtä käsittelevässä Vuoripoika Oy:ssä.

Ratkaisuvaihtoehtoja tietoverkon uudistukselle on kaksi, riippuen siitä minkälainen tietoverkon pohjaratkaisu tytäryhtiössä on. Ensimmäinen vaihtoehtoehto sopii Vuoripoika Oy:hyn tai TMT. Malinen Oy:n tytäryhtiöihin, joissa on olemassa oleva internetyhteys. Toinen vaihtoehto sopii tilanteeseen, jossa halutaan toteuttaa verkko modeemista lähtien omilla päätelaitteilla.

Vaikka lopputulos molemmissa ratkaisuissa on sama, kannattaa tietoverkon uudistus toteuttaa ensimmäisellä vaihtoehdolla, koska se on helpommin siirrettävissä ja monistettavissa. Vaihtoehdon yksi palomuuripäätelaite voidaan asentaa olemassa olevaan lähiverkkoon, ja tulevaisuudessa siirryttäessä uusiin tiloihin tai internetyhteyden vaihtuessa saadaan VPN-yhteys toimimaan ilman suurempia konfigurointeja tai viiveitä.

WLAN-kanavien mittaukset osoittivat muutamien WLAN-kanavien olevan ruuhkaisia, joten tietoverkon uudistuksen yhteydessä mitata. Vuoripoika Oy:n tietoverkon laajennuksen yhteydessä WLAN-verkon kanavaksi tulee valita mittauksissa todettu ruuhkattomin kanava, esimerkiksi 4, 5, 7, 8, 9, 10, 12 tai 13.

Toteutuksen läpiviemiseksi tehtyyn listaan (taulukko 8) on kerätty hankittavat päätelaitteet, sekä merkitty mahdollinen konfigurointi tarve, jotta järjestelmä

saadaan toimimaan. Lista on suurpiirteinen, ja uudistuksen toteuttajaksi on järkevää käyttää tietoverkosta vastaavaa konsulttiyhtiötä.

TAULUKKO 8. Uudistussuunnitelmassa hankittavat tai konfiguroitavat päätelaitteet

	Palomuuripäätelaite	WLAN-tukiasema	ADSL-modeemi	Palomuuripäätelaite
Merkki ja malli	Zyxel USG 20W	Zyxel WAP3205	Cisco 887VAE	
Uushankinta	X	X	-	-
Kappalemäärä	1	3	-	-
Konfigurointitarve	X	X	X	X
TMT. Malinen Oy	-	-	-	X
Vuoripoika Oy	X	X	X	-

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Opinnäytetyössä selvitettiin kohdeyrityksen erilaisia ratkaisuvaihtoehtoja lähiverkon laajentamiseksi yrityksen tytäryhtiöihin. Vertailtavien vaihtoehtojen tuli olla edullisia sekä helposti monistettavia, mutta tietoturva- sekä VPN-ominaisuuksiltaan nykyaikaisia. Monistettava ja helposti siirrettävä ratkaisu saisi olla langaton tai mahdollisimman vähän kaapelivetoja vaativa kokonaisuus.

Työssä päätyttiin tarjoamaan kahta ja suosittelemaan yhtä vaihtoehtoa, koska toinen ratkaisu voi olla parempi yhtiön toisessa toimipisteessä kuin toinen. Vaihtoehto yksi toimii olemassa olevassa verkossa ja vaihtoehto kaksi sopii tilanteeseen, jossa modeemi vaihdetaan VPN-tunnelointeja tukevaksi. Kummassakin vaihtoehdossa muodostetaan VPN-tunneli TMT. Malinen Oy:n ja Vuoripoika Oy:n välille, ja VPN-tunnelin avulla saadaan TMT. Malinen Oy:n lähiverkko jaettua Vuoripoika Oy:hyn. Vuoripoika Oy:ssä lähiverkko jaetaan WDS-tuella olevien WLAN-tukiasemien avulla tuotanto- ja toimistotiloihin.

Opinnäytetyön teon aikana Vuoripoika Oy:n ADSL-yhteyttä oli parannettu ja DNA Oy:n vuokramodeemi oli vaihdettu CISCO:n 887VAE:ksi. Modeemi on erittäin laadukas, ja harkittavaksi jää, halutaanko kustannussyistä vuokramodeemia konfiguroida niin, että sillä toteutettaisiin vaihtoehdossa kaksi esitetty ratkaisuvaihtoehto.

Kohdeyrityksen tietoverkkoa ja tietoturvaa ylläpitää maksullinen konsulttiyhtiö, ja työ ei otakaan kantaa siihen, mitä muutoksia pitäisi tehdä tietoturvan osalta. Tietoverkon laajennussuunnitelma on pyritty tekemään siltä pohjalta, että tietoturva on oikealla tasolla eivätkä työssä suositellut uudistukset aiheuta aukkoja olemassa olevaan tietoturvaan. Tietoturvan parantamiseksi suositellaan tietoturvakoulutusta kaikille yhtiön työntekijöille – ensisijaisesti niille, jotka työskentelevät yhtiön tietokoneilla.

Opinnäytetyössä käsitellyn ratkaisun pohjalta olisi hyvä tehdä toteutus, joka raportoitaisiin, ja näin mahdolliset kysymykset tai selvittämättä jääneet asiat tulisivat esille. Raportointi helpottaisi myös ratkaisun monistamista kohdeyrityksen muihin tuotanto- ja toimistotiloihin. Työn selkeä ja hyvä

raportointi auttaisi myös tulevaisuudessa, jos yrityksen henkilökunta tai IT-konsulttiyritys vaihtuu.

Järkevää olisi myös selvittää yrityksen tietoturvaratkaisujen ajantasaisuus perinpohjaisesti ja antaa suosituksia, jotka palvelisivat yritystä sen kasvaessa tai muuttuessa ja tietoverkkoratkaisujen kehittyessä. Tietoturvaratkaisujen selvityksen yhteydessä voitaisiin järjestää yhtiön työntekijöille yleinen tietoturvakoulutus sekä antaa ohjeita etätyöasemia käyttäville työntekijöille.

Yrityksissä tietotietoverkko- ja tietoturvaratkaisut on toteutettu eritasoisella osaamisella ja helposti tietoverkkoratkaisuihin ei haluta yrityksissä investoida minimiä enempää. Asiantuntijan opastuksella toteutettu tietoverkkoratkaisu ei välttämättä ole kallis, mutta ulkopuolisen ja puolueettoman asiantuntijan konsultaatio on järkevää, jos itse ei tunne erilaisia tietoverkkoratkaisuja tarpeeksi hyvin. Nopea, turvallinen ja joustava tietoverkkoratkaisu hyödyttää yritystä ja tehokkaasti käytettynä voi parantaa myös yrityksen tuottavuutta.

LÄHTEET

Boyle, R. & Panko R. 2013. Corporate Computer and Network Security. Third edition. New Jersey: Pearson Education Inc.

Cisco. 2013. Network Address Translation (NAT) FAQ 2013 [viitattu 14.7.2014]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A., Ritchey, R. & Sahrma, S. 2005. Guide to IPsec VPNs. NIST Special Publication 800-77 [viitattu 20.7.2014]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

Funet. 2014. WLAN-verkon tietoturva [viitattu 14.8.2014]. Saatavissa: https://info.funet.fi/wiki/display/avoin/BCP+WLAN-verkon+tietoturva

Geijer, J. 2004. Langattomat verkot. Helsinki: Edita prima Oy.

Google. 2014. Google Maps [viitattu 28.8.2014]. Saatavissa: https://www.google.fi/maps

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. Helsinki: Edita Prima Oy.

Korpela, J. 2005. Kodin tietoturvaopas. 1. painos. Jyväskylä: Docendo Finland Oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Suomicom. 2014. Laajakaistavertailu [viitattu 22.7.2014]. Saatavissa: http://www.suomicom.fi/laajakaistavertailu/

Tallinna Ülikooli. 2014. Lähiverkot [viitattu 22.7.2014]. Saatavissa: http://www.tlu.ee/~matsak/telecom/lasse/Data_networks/lhiverkot.html

Luoti. 2005. Mobiilimaailman tietoturvauhat ja ratkaisut 2005 [Viitattu 24.7.2014]. Saatavissa: http://www.lvm.fi/fileserver/1_2005.pdf

TMT. Malinen Oy. 2014. [viitattu 7.7.2014]. Saatavissa: www.TMT.fi

Porras, J. 2014. Luento 8 – Wi-Fi [viitattu 14.8.2014]. Saatavissa: http://www2.it.lut.fi/kurssit/08-09/CT30A2600/luennot/CT30A2600%20luento8%20WLAN.pdf

Verkkokauppa. 2014. [viitattu 25.7.2014]. Saatavissa: www.verkkokauppa.com

Wikipedia. 2014a. GRE [viitattu 2.11.2014]. Saatavissa: http://fi.wikipedia.org/wiki/GRE

Wikipedia. 2014b. HSDPA [viitattu 16.11.2014]. Saatavissa: http://fi.wikipedia.org/wiki/HSDPA

Wikipedia. 2014c. Kaapelimodeemi [viitattu 16.11.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Kaapelimodeemi

Wikipedia. 2014d. Parikaapeli [viitattu 2.11.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Parikaali

Wikipedia. 2014e. SHDSL [viitattu 14.9.2014]. Saatavissa: http://fi.wikipedia.org/wiki/SHDSL

Wikipedia. 2014f. SSL VPN [viitattu 21.7.2014]. Saatavissa: http://fi.wikipedia.org/wiki/SSL_VPN

Wikipedia. 2014g. Tietoturva [viitattu 7.7.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Tietoturva

Wikipedia. 2014h. VPN [viitattu 17.7.2014]. Saatavissa: http://fi.wikipedia.org/wiki/VPN

Wikipedia. 2014i. Virustorjunta [viitattu 20.7.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Virustorjunta

Wikipedia. 2014j. WLAN [viitattu 15.7.2014]. Saatavissa: http://fi.wikipedia.org/wiki/WLAN

Wikipedia EN. 2014. WDS [viitattu 20.7.2014]. Saatavissa: http://en.wikipedia.org/wiki/Wireless_distribution_system

Windows Server. 2008. VPN Tunneling Protocols [viitattu 27.7.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx